Securing Service-Oriented and Event-Driven Architectures
Results of an Evaluation of Enterprise Security Frameworks

Heiko Klarl
University of Regensburg and iC Consult GmbH
hklarl@klarl.eu

Markus Preitsameter
University of Applied Sciences Regensburg
markus@preitsameter.de

Abstract

With the emerging trend to (re-) design IT-systems as service-oriented and event-driven architectures new security paradigms are required. This position paper describes the various threats and measures against them. On this base evaluation results of securing a business process are presented. An outlook on future research work on combining Model-Driven techniques and security requirements on a higher modeling level will conclude the paper.

Keywords: *Service Oriented Architecture (SOA), Event Driven Architecture (EDA), Security, Securing business processes, Model driven security*

1. Introduction

The success of the Internet, the ongoing globalization and the implementation of new compliance regulations like Basel II and Sarbanes-Oxley Act led to a demand for new solutions to meet the requirements for IT-systems. The paradigm of service-oriented (SOA) and event-driven architectures (EDA) with fine grained and loosely coupled services tries to cope with those needs. The distributed system works in an asynchronous way and service providers and consumers are decoupled and don't depend on the availability of specific services.

2. Security threats within SOA and EDA

Every security threat in SOA and EDA environments can be aggregated by a single threat or a combination of three basic security threats [1]: *unauthorized access to information*, *unauthorized modification of information* and *unauthorized modification of functionality.* Different measures such as digital signatures and public key cryptography as well as authentication and authorization techniques can successfully cope with those threats [2].

3. Securing the business case

In [2] two frameworks securing a business process of a German Bank were evaluated. First the process had to be re-designed according to the SOA paradigm. Additionally, security considerations were made that resulted in an informal description of security policies for authentication, authorization and message exchange.

For securing the business case, two different products were chosen. BSF [3] uses proxy-like interceptors. It supplies message security and certificate based service authentication and authorization. The policies could be implemented with the help of a graphical designer. The portal layer, which is the front-end for all user interactions, was secured by ALES [4] which controls access to the different resources like URLs, EJBs or simple webpages. Security policies can be created by combining users or roles, resources and access rights in a reasonable manner to fit the formulated security requirements.

4. Future research work

Business processes could be designed in a very abstract way, but the creating of security policies is still independent from the models. This leads to the problem, that a software architect is modeling the business process, whereas the IT security department, which is possibly not very familiar with the business process, has to secure the process. Due to a lack of knowledge about what the business process is doing and what actually should be secured, the risk of having an inadequately secured business process is very high. It could be reduced by using model driven approaches which deduce security policies from models combined with the usage of business security patterns (cf. [5]). A close coupling of the model and its security requirements will cause a consistent state across all changes in the business process and bind the security administration stricter to the development process. Finding ways to add this kind of information to the different modeling approaches e. g. UML will be a part of future research work.

References

[1] GEER, D.: Taking Steps to Secure Web Services. In: *Computer* 36 (2003), Oct., Nr. 10, p. 14–16
[2] KLARL, H. et al.: *Evaluierung von Sicherheitsframeworks für serviceorientierten Architekturen*, UAS Regensburg, 2006
[3] BESEQURE GMBH: *Business Security Framework (BSF)* http://www.besequre.com/en/Framework/index.php, 2006
[4] BEA SYSTEMS, INC.: *BEA AquaLogic Enterprise Security*, http://bea.com/ales, 2005
[5] IMAMURA, T. et al.: Patterns for Securing Web Services Messaging, In: *OPSLA Workshop on Web Services and Service Oriented Architecture Best Practice and Patterns, 2003*